Defense Intelligence Agency

Department of Defense Intelligence Management System

Accreditation Test Procedures

Prepared For:
DoDIMS PMO
National Intelligence Production Center
DIA/PO-5C

Prepared By:
J.G. Van Dyke & Associates, Inc.
6550 Rock Spring Drive, Suite 360
Bethesda, Maryland 20817

November 14, 1994

FOREWORD

The Department of Defense Intelligence Management System (DoDIMS) Accreditation Test Procedures is being written as part of a generic set of accreditation documentation to support accreditation of DoDIMS at specific user sites. Each site will need to review this documentation and modify it, as necessary, to address specific site environment in which DoDIMS will operate.

Table of Contents

Section **Page**

Section **Page**

1.0 **Purpose**

1.1 **Purpose of Accreditation Testing**

Accreditation testing will confirm the existence and functionality of the safeguards identified in the Defense Intelligence Agency (DIA) Department of Defense (DoD) Intelligence Management System (DoDIMS) Security Concept of Operation (SECONOPS). In doing so, it will determine that the system satisfies the established security requirements for processing sensitive intelligence information for the System High mode of operation.

1.2 **Purpose of the Test Procedures Document**

The DIA DoDIMS Accreditation Test Procedures document is the consolidation of individual test procedures and steps which will be performed at the time of accreditation testing. It will provide: (1) the test steps within each procedure and (2) a Security Requirements compliance Matrix (SRCM) that maps security requirements to test sets and test procedures.

2.0 **References**

The following two paragraphs contain a list of reference documents used to support accreditation of DoDIMS for processing of Sensitive Compartmented Information (SCI). These documents provide additional sources of information concerning various aspects of DoDIMS and the accreditation process.

2.1 **System Documentation**

The following DoDIMS documents provide descriptive information upon which the accreditation of DoDIMS will be based.

a. DoDIMS Security Concept of Operations (SECONOPS).

b. DoDIMS System Security Requirements (SSR).

c. DoDIMS Threat Assessment.

d. DoDIMS System Security Analysis (SSA).

e. Information System Security Officer (ISSO) appointment letter.

f. SunOS System and Network Administration Manual, Sun Microsystems,1991.

2.2 **DoD Documents**

The following list contains documents which provide supportive information for the accreditation process and its requirements:

a. DIA Manual (DIAM) 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities, FOR OFFICIAL USE ONLY

b. DIAM 50-4, Security of Compartmented Computer Operations, CONFIDENTIAL, 24 June 1980

c. DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, unclassified, 26 December 1985

d. DIA Regulation (DIAR) 50-37, Control of Computer Output and Verification of Computer Output Classification for Compartmented Computer Operations, unclassified, 24 March 1987

e. DoD Directive C-5200.5, Communications Security (COMSEC), CONFIDENTIAL, 15 April 1971, as amended

f. MIL-HDBK-232, Military Standardization Handbook RED/BLACK Engineering--Installation Guidelines, 14 November 1972

g. DoD Directive S-5200.19, Control of Compromising Emanations, SECRET, 10 February 1968, as amended

h. DCID 1/16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks, SECRET--REL UK/CAN/AUS, 19 July 1988

i. DoD C-5030.58-M, Defense Special Security Communications System Security Criteria and Telecommunications Guidance, CONFIDENTIAL, July 1978

j. DOI-103, Defense Special Security Communications System (DSSCS) Operating Instructions, System/Data Procedures, CONFIDENTIAL, January 1983

k. NACSIM 5100, Compromising Emanations Laboratory Test Standard Electromagnetics, unclassified

l. DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), unclassified, 21 Mar 1990

m. DIAM 50-XX, DIA Security Handbook for Automated Information Systems and Separately Accredited Networks (Draft), SECRET, 14 Dec 1990

3.0 **General System Description**

3.1 **Mission Supported**

DoDIMS is a software application designed to support the DoD and National intelligence communities in registering, validating, tracking and managing production requirements. It provides the mechanism for scheduling, deconflicting, tasking production and most importantly, provides the capability to track and manage overall production activities across operational and national planners and consumers.

3.2 **System Functionality**

DoDIMS performs 3 basic functions: 1) register Production Requests and Intelligence Products initialization/updates; 2) replicate data to DoDIMS sites; and 3) update the peer databases and Central Database.

3.3 **System Architecture**

DoDIMS is a client-server application developed in accordance with DoD and DIA information system architectural standards. It consists of five client modules which reside on a JDISS workstation and a database co-hosted on the workstation. Eventually a master, read-only database will be established on a dedicated server at the DIAC.

3.3.1 **Hardware**

DoDIMS currently utilizes a JDISS workstation to host both client application modules and a server database. All systems will be based on a standard JDISS configuration. The hardware for the master database to be installed at the DIAC is to be determined. The standard configuration is as follows, however, *site specific configurations may differ*:

- Sun SPARCStation 2/10/20 with 32 or 64 MB RAM
- Sun High Resolution Color Monitor
- Sun CD-ROM Drive
- 1.3 GB internal or 2.1 GB external hard drives (minimum)
- Ethernet Transceiver
- Two (2) serial ports
- Bi-directional Printer Port
- 8mm Tape Drive
- Mouse
- NeWSprinter CL+ Color Printer

3.3.2 **Software**

DoDIMS/JDISS software consists of both commercial-off-the-shelf software, DoDIMS- unique software developed under Government contract and Government-Furnished software

3.3.2.1 **COTS Software**

COTS software consists of the following

- SUN OS 4.1.3
- X-windows X11.R5
- OSF Motif 1.2
- Looking Glass Professional 3.0
- ApplixWare 2.1
- ELT/2 2.2.10-R4 with TACO2
- Open Connect TN3270 with graphic option
- TEEMX
- XNVDET
- Sybase 10.0.1
- Sybase Replication Server 100.1
- Gain Momentum Runtime
- Newsprint

3.3.2.2 **DoDIMS-Unique Software**

3.3.2.2.1 **Client Software**

DoDIMS-unique client software is in the application written in Gain Extension Language (GEL) to provide the following modules:

a. Requirements Module. This module provides the user with an automated Production Requirements (PR) process in support of both crisis and non-crisis requests. It provides the intelligence consumer a mechanism to register production requirements and forward them to the appropriate validating organization and, where applicable, any additional authorities. Once validation occurs, a production center is notified of the PRs existence. After reviewing the PR, and coordinating with collaborative production centers if appropriate, the production center sends the consumer a response on the proposed production actions. At any given time, a customer and/or validator has the ability to track the status of the PR through its organization and to the producing organization.

b. Assignment Module. As production requirements are fully validated, this module will automatically enter the responsible production center information for assignment based on

geographical and functional areas. For requests comprising more than one responsible producer areas, the validator will select primary and collaborative producers. This final validating authority is empowered to override the assignment criteria as necessary. DoDIMS will not assign production without an appropriate link to a validated requirement to ensure production resources are being utilized to satisfy consumer requirements.

c. Production Module. This module makes available to the community an on-line production schedule. Production center production managers will have the ability to input and maintain their annual scheduled production. In addition, deconfliction will be accomplished as new information is submitted. An individual entering data will review perceived duplicate entries prior to submitting a new request, or initiating an intelligence product. As products are published and production schedule records closed-out, cross-reference information will be available to assist the user in retrieving the publication through DoDIIS Dissemination.

d. Reports Module. This module makes available to its users a capability to obtain production management information by utilizing either various pre-defined or user-defined reports. Whatever the type of report, a graphics capability is available consisting of Pie, Bar, Area, line column, 3-D types of charts.

e. Assessment Module. This module provides a mechanism by which primarily production managers and functional managers obtain information regarding resource utilization, producer assessments, and production shortfalls.

3.3.2.2.2 **Server Software**

DoDIMS server software consists of data tables developed within Sybase.

3.3.2.2.3 **Government Furnished Software**

JINTACCS Automated Message Processing Software (JAMPS)

3.3.3 **Firmware**

There is no DoDIMS-unique firmware.

3.3.4 **Communications**

DoDIMS will use data networking and communications associated with the JDISS workstation. In most cases, the workstation will be attached to a dedicated LAN which will connect to JWICS or connect to a site LAN which will connect to JWICS.

3.3.5 **Information Flow**

3.3.5.1 **Inputs**

DoDIMS will receive input primarily from the user community. Users will be categorized as Requestors, Validators, and Production managers. User inputs will range in classification from unclassified to TS/SI/TK depending on the nature of the production request and/or query. User input will update the database by direct keyboard interface, mouse activation, and indirectly by the application environment, e.g., cut and paste. Updates of the database will be performed as a system administration function. Inputs for updating system tables will be by file transfer protocol (FTP), floppy diskette or 8mm tape.

3.3.5.2 **Outputs**

The principal output will be visual via a display monitor. The classification level will be permanently displayed on each workstation defaulted to the highest classification level processed by the application. All hard copy output will be appropriately labeled at the top and bottom of each page.

Transactions, i.e., production requests, will be replicated by the COTS database software to applicable DoDIIS sites via JWICS/JDISS. Transaction replication will also be made to both peer databases and the central DoDIMS server resident in the DIAC. Should communication downtime occur, output to the central server will be stored and forwarded by each site's replication process upon re-establishment of the communication link.

3.3.3.3 **Sanitization/Decompartmentation**

DoDIMS will not accomplish sanitization or decompartmentation

3.3.3.4 **Access by Foreign Nationals**

There will be no access by foreign nationals.

4.0 **System Testing**

The DoDIMS Accreditation Test Plan provides a complete description of events that will occur before, during, and after the execution of the test. However, the following paragraphs will provide specific information about the execution of the test procedures.

4.1 System Test Environment

The DoDIMS accreditation test is being conducted using site specific software, databases, and communications. Unclassified test data is used.

4.2 System Test Constraints/Assumptions

The DoDIMS test procedures attempt to emulate situations encountered during normal system operations. No constraints existed in attempting to create an operational environment for testing. The system was considered to be fully functional and operational for the test. These test procedures were intended to validate security features. Functional testing for system acceptance is assumed to have been successfully completed prior to accreditation testing. It is also assumed that all accreditation test procedures were successfully executed in a "pre-test" prior to actual accreditation testing.

4.3 Test Progression

In formulating the test procedures, an effort was made to minimize the repetition of certain system functions in the performance of separate tests. The sequence of the test procedures will be identified on each test procedure. Because of this, adherence to the order of tests described within each functional area is suggested.

4.4 Test Execution

Paragraph 1.1 of the DoDIMS Accreditation Test Plan states that the accreditation is based on a field review which includes: (1) inspection of required security related documents, (2) execution of the System Accreditation Test Procedures, and (3) assessment of the proficiency of site operations personnel. Inspection of security related documents is performed by the Test Director, generally prior to the start of the actual test. During test execution the Test Director will assess the overall proficiency of site operations personnel, normally rotating responsibilities to ensure operational integrity. This DoDIMS Accreditation Test Procedures document contains the step-by-step instructions and is the means by which the Test Director is assured that all security requirements are tested.

The accreditation test is under the direct control of the Test Director at all times, and the Test Director is responsible to ensure that all tests are performed correctly and the expected results are obtained. A detailed check must be performed of all test results. Nothing is "assumed". This check is normally a visual inspection and is accomplished by comparing test output(s) to the expected results identified in the test procedure. The result of this comparison determines success or failure of that particular test. Before a test is declared a failure based upon unexpected results, the Test Director must ensure that the error is not document related. If the observed output is identical to the expected result (other than expected specified exceptions such as date and/or time) then the test is determined

to be successful and the test being documented, if required. Any result other then the "expected" must be analyzed to determine whether a failure has occurred or whether the expected result in the test procedure is in error. If the latter occurs, the proper annotations must be made in the Test Procedure document. If the test step has been determined to be a failure, further analysis must be performed to determine if retesting immediately is feasible, if retesting must occur at a later time, or if the test failure is catastrophic enough to discontinue testing at this time. In all cases the proper annotations must be made in the Test Log and/or Test Procedures document.

5.0 **System Test Procedures**

Appendix C contains the specific Test Procedures which correspond to the test sets as identified in the SRCM in Appendix B. These test procedures will be used by the Test Director and the test team to perform the DoDIMS accreditation testing.

APPENDIX A

Terms and Abbreviations

AIS	Automated Information System
COMSEC	Communications Security
COTS	Commercial Off-the-shelf
DAA	Designated Approving Authority
DCID	Director of Central Intelligence Instruction
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIAM	DIA Manual
DIAR	DIA Regulation
DoD	Department of Defense
DoDIMS	Department of Defense Intelligence Management System
DOI	DSSCS Operating Instruction
DSSCS	Defense Special Security Communications System
EPL	Evaluated Products List
ISSO	Information System Security Officer
JAMPS	JINTACCS Automated Message Processing System
JDISS	Joint Deployable Intelligence Support System
JINTACCS	Joint Interoperable Automated Command and Control System
JWICS	Joint World-wide Intelligence Communications System
LAN	Local Area Network
PMO	Program Management Office
PR	Production Requirement
SCI	Sensitive Compartmented Information
SECONOPS	Security Concept of Operations
SRCM	System Requirements Compliance Matrix
SSA	System Security Analysis
SSR	System Security Requirements
TBD	To be determined

APPENDIX B

SECURITY REQUIREMENTS COMPLIANCE MATRIX

Security Requirement	Security Requirement Title	Test Number
1a	Conceptual Design	1a
1b	Mode of Operation	1b
1c	Identification of Accrediting Authority	1c
2	System Security Plan	2
3	Appointment of ISSO	3
4	Access by Foreign Nationals	4
5	Accreditation/Reaccreditation	5
7	Interim Approval to Operate	7
8	Security Briefings	8
10	Protection of High Density/Transportable Storage Devices	10
11	Memory Remanence	11
12	Protected Software and Hardware	12
14	Marking Storage Media	14
15	Marking Printed Output	15
16	Manual Review of Human Readable Output	16
17	System Disposal Plan	17
18	COMSEC	18
20	TEMPEST	20
21	Physical Security	21
22	Personnel Security	22

23	Commercial Vendor Maintenance	23
25.a	Discretionary Access Control	25.a
25.b	Object Reuse	25.b
25.c	Identification and Authentication	25.c
25.d	Audit	25.d
25.e	System Architecture	25.e
25.f	System Integrity	25.f
25.g	Security Testing	25.g
25.h	Security Features User's Guide	25.h
25.i	Trusted Facility Manual	25.i
25.j	Test Documentation	25.j
25.k	Design Documentation	25.k
25.l	Identification of User Terminals	25.l
25.m	Configuration Management	25.m
25.n	Trusted Distribution	25.n

APPENDIX C

DoDIMS Security Test Procedures

DoDIMS Mode of Operation Test Procedure
(Test 1.a)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the conceptual design of DoDIMS was developed using a systems engineering approach.	Review the conceptual design of DoDIMS.	DoDIMS conceptual design use a systems engineering approach .			

DoDIMS Mode of Operation Test Procedure
(Test 1.b)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the Mode of Operation of DoDIMS is operating in System High mode.	Review the Mode of Operation Plan.	Mode of Operation Plan requirements are met.			

DoDIMS ID of Accrediting Authority Test Procedure
(Test 1.c)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the ID Accrediting Authority document for DoDIMS is DIA/DSM-SIM.	Review the Accrediting Authority document.	Accrediting is DIA/SY-1D.			

DoDIMS System Security Plan Test Procedure
(Test 2)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify DoDIMS has a System Security Plan.	Review the System Security Plan.	The System Security Plan has been written and satisfies the requirements of DCID 1/16.			

DoDIMS Appointment of ISSO Test Procedure
(Test 3)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the Appointment of the DoDIMS ISSO.	Review the Appointment Letter for the ISSO.	ISSO is appointed.			

DoDIMS Access by Foreign Nationals Procedure
(Test 4)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify that Foreign Nationals do not have access to DoDIMS	Review Access Control procedures.	Procedures are in place to preclude Foreign Nationals from accessing DoDIMS.			

DoDIMS Accreditation/Reaccreditation Procedure
(Test 5)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Accreditation/Reaccreditation.	Review all System security documents.	All documents should comply with minimum requirements established by the DAA. Documents should describe all aspects of the system's operations and security functions. System will specify reaccreditation requirements.			

DoDIMS Interim Approval to Operate Test Procedure
(Test 7))

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify that DoDIMS satisfies minimum requirements for interim approval to operate.	Review System Security Plan.	System Security Plan satisfies requirements for DoDIMS to obtain interim approval to operate.			

DoDIMS Security Briefing Test Procedure
(Test 8)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify users receive initial and periodic refresher training on ADP security.	Review security training records.	Users receive initial and periodic refresher training on ADP security.			

DoDIMS Protection of High Density/Transportable Storage Devices Test Procedure
(Test 10)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the Protection of High Density and Transportable Storage Devices for DoDIMS.	Review Security Plan for written procedures on the protection of High Density and Transportable Storage devices.	The requirements for protecting High Density and Transportable devices are met.			
2.	Verify backup storage media, such as tapes and disks are protected from unauthorized removal from the secure environment.	Backup media should be stored in the computer room or in a location protected at a level at least equal to that of the computer room.	A tape library is set up to record all tapes or disks on a log.			
3.	Verify backup storage media of all sensitive files are being compressed then encrypted to protect the information if the media is lost.	Review procedures and ensure "Compress" and "Crypt" commands are being used.	"Compress and "Crypt" commands are being used to protect backup media.			

DoDIMS Memory Remanence Test Procedure
(Test 11)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the procedure of handling memory remanence for DoDIMS.	Review Security Plan for written procedures on the protection and handling procedures of memory remanence.	The requirements for protecting and or handling memory remanence is met.			
2.	Verify the procedure of controlling memory remanence for DoDIMS.	Review Security Plan for written procedures on controlling of memory remanence.	The requirements for controlling memory remanence is met.			
3.	Verify the procedure to destroy memory remanence for DoDIMS.	Review Security Plan for written procedures on destroying memory remanence.	The requirements for destroying memory remanence is met.			
4.	Verify the procedure to release memory remanence, (magnetic storage media) for DoDIMS.	Review Security Plan for written procedures on releasing memory remanence.	The requirements for releasing memory remanence is met.			

DoDIMS Protected Software and Hardware Test Procedure
(Test 12)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the procedure for protected software for DoDIMS.	Review Security Plan for written procedures on the protection of Software.	The requirements for protecting DoDIMS software is met.			
2.	Verify the procedure for protected system hardware for DoDIMS.	Review Security Plan for written procedures on the protection of DoDIMS Hardware.	The requirements for protecting DoDIMS Hardware is met.			

DoDIMS Marking Storage Media Test Procedure
(Test 14)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the procedure for marking removable media with external labels identifying the proper sensitivity and handling restrictions for DoDIMS.	Review Security Plan for written procedures on the marking of storage media.	Written procedures pertaining to storage media for DoDIMS meets all requirements.			
2.	Verify magnetic storage media, (tapes, diskettes, hard drives) are marked with the highest classification.	Review Security Plan for written procedures on the markings of magnetic storage media, (tapes, diskettes or hard drives).	All magnetic media, (tapes, diskettes, and hard drives are all properly labeled with the highest classification required.			

DoDIMS Marking Printed Output Test Procedure
(Test 15)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the procedure for marking printed output.	Review Security Plan for written procedures on the marking of printed output.	Written procedures pertaining to marking printed output for DoDIMS.			
2.	Verify the beginning page (security banner page) with a human readable label of the systems accredited security parameter and include appropriate warning message concerning classification and control of the output.	Print off cover page and review for security banner and markings.	Security banner is printed off as the first page of the document and all security makings are present.			
3.	Verify individual pages are marked to reflect the appropriate classification, controls and handling restrictions.	Print off document and review for classification markings on the required pages and handling restrictions.	Printed document has the required markings on all pages and the handling notice is printed.			
4.	Verify the procedure for marking printed output from screen prints.	Review classified material on CRT. Perform a screen print of displayed information being displayed.	Classified screen prints should have the classification marking of the highest information contained within.			

DoDIMS Manual Review of Human Readable Output Test Procedure
(Test 16)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the procedure to provide reliable human review of output from a system with untrusted markings or labels.	Review Security Plan for written procedures on the procedure to verify untrusted markings on printouts.	Written procedures pertaining to reviewing markings on printed output for DoDIMS are met.			
2.	Verify the procedure for marking printed output from screen prints.	Review classified materia on CRT. Perform a screen print of displayed information being displayed.	All classified screen prints should have the classification marking of the highest information contained within.			

DoDIMS System Disposal Plan Test Procedure
(Test 17)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the procedure for System Disposal of software.	Review Security Plan for written procedures on the disposal plan of system software.	Written procedures pertaining to System Disposal of DoDIMS software are met.			
2.	Verify the procedure for disposal of System printed output.	Review written procedures covering disposal of system printed output.	Written procedures pertaining to System Disposal of printed output of DoDIMS are met.			

DoDIMS COMSEC Test Procedure
(Test 18)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify DoDIMS system compliance with all applicable COMSEC regulations and local policies for systems handling Top Secret SCI material.	Review written procedures and regulations to ensure DoDIMS is in compliance.	Written procedures pertaining to handling Top Secret SCI material meet all COMSEC requirements.			

DoDIMS TEMPEST Test Procedure
(Test 20)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify DoDIMS system compliance with the National Policies and local DIAC regulations on compromising emanations.	Review National Policies and local DIAC regulations and verify DoDIMS is meeting those requirements.	DoDIMS is in compliance with the National Policies and local DIAC regulations.			
2.	Verify Red/Black separation of power lines.	Review layout of Red/Black power lines.	DoDIMS passes Red/Black separation.			
3.	Verify communication lines are separated from electrical lines.	Review layout of communication lines and electrical lines.	Communication lines and electrical lines are separated by the required distance.			
4.	Verify filtered power (if required).	Verify DoDIMS is on filtered power.	TBD			
5.	Verify the systems in operation are meeting separation requirements or are on the Evaluated Product List (EPL).	Review EPL to determine if systems in operation are meeting separation requirements.	Systems are on the EPL or are meeting the separation requirements.			

DoDIMS Physical Security Test Procedure
(Test 21)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the physical security of all DoDIMS components meet the requirements for processing SCI information.	Review all DoDIMS system components and ensure they meet the physical requirements for processing SCI information.	DoDIMS meets all physical security requirements.			

DoDIMS Personnel Security Test Procedure
(Test 22)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify all DoDIMS users are cleared.	Review documentation that all individuals with access to DoDIMS are cleared.	All DoDIMS users are cleared.			
2.	Verify all DoDIMS users are approved for access.	Review documentation that all individuals are approved for DoDIMS access.	All DoDIMS users have the approved access.			
3.	Verify individuals have the appropriate need to know approvals for all data processed by or stored within the system.	Review documentation that all individuals have the appropriate need to know to have access to all data on the DoDIMS system.	All individuals have the appropriate need to know for all data processed or stored within DoDIMS.			

DoDIMS Commercial Vendor Maintenance Test Procedure
(Test 23)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify DoDIMS compliance with regulations requiring specific controls for system access by commercial maintenance personnel.	Review Security Plan for written procedures pertaining to access controls for maintenance personnel.	Written procedures pertaining to maintenance personnel meet all requirements.			
2.	Verify a visitor log is being utilized.	Review visitor log procedures.	Visitor log is being utilized for DoDIMS.			
3.	Verify visitor badges are being utilized.	Review visitor badge procedures.	Visitor badges are being used for DoDIMS.			

DoDIMS Discretionary Access Control Test Procedure
(Test 25.a)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify all users are required to identify themselves and provide an authentication mechanism prior to being allowed to access the system.	Attempt to login to an approved workstation as user1, user2, and user3 using correct users ID's and passwords.	All logins are successful.			
		Attempt to login on an approved workstation as user1, user2, and user3 using incorrect passwords (i.e., random keystrokes).	All login attempts are unsuccessful.			
		Attempt to login on an approved workstation using a random incorrect user ID and a random password.	The attempt is unsuccessful.			
2.	Verify that all users are identified when they access DoDIMS.	Start DoDIMS from an approved workstation as user1, user2, and user3. (user1, user2, and user3 are all valid DoDIMS users).	Attempt successful.			
		Start DoDIMS from an approved workstation as user4, user5, and user6. (user4, user5, and user6 are not valid DoDIMS users)	Attempt unsuccessful.			

3.	Verify Discretionary file access. Attempt to gain information from records that a user has not been granted access.	Attempt to view record for which user has not been granted access.	Attempt unsuccessful.
		Attempt to view record for which user has been granted access.	Attempt successful.

DoDIMS Object Reuse Test Procedure
Test 25.b)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify user4 Object area is not accessible to other user.	Login as user4 Attempt to view Object area (directory).	Login is successful. Attempt is unsuccessful.			

DoDIMS Identification & Authentication Test Procedure
(Test 25.c)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify all users are required to identify themselves and provide an authentication mechanism prior to being allowed to access the system.	Attempt to login to an approved workstation as user1, user2, user3 using the correct user ID's & passwords.	All logins are successful.			
		Attempt to login to an approved workstation as user1, user2, and user3 using incorrect passwords (i.e., random keystrokes).	All login attempts are unsuccessful.			
		Attempt to login to an approved workstation using a random incorrect user ID, and a random password.	The attempt is unsuccessful.			
2.	Verify each individual user is identified by DoDIMS as to what records the user has been granted and what capabilities the user has.	Logon to an approved workstation as user1. Start the DoDIMS application. Attempt to view a record that user1 has not been granted access to.	Attempt unsuccessful.			
		Logon to an approved workstation as user1. Start the DoDIMS application. Attempt to view a record for which user1 has been granted.	The attempt is successful.			

DoDIMS Audit Test Procedure
(Test 25.d.1)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Initialize DoDIMS server C2 audit function.	Login as DoDIMS server Unix SA.	Successful login			
		Reset the audit log files from the audit user interface.	Audit files successfully reset.			
		Change the events audited by the system to include the following system events: data_read, data_write, data_create, data_access_change, login_logout, administrative, minor_privilege, major_privilege.	Audit successfully changed to include desired events to be audited.			

DoDIMS Audit Test Procedure
(Test 25.d.2)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify Unix OS audit data should be protected from modification and unauthorized destruction and should be readable only by authorized individuals.	At the conclusion of security testing and after other audit tests are completed, login as ISSO and make backups of the DoDIMS server C2 audit files	Backups successfully made.			
		Attempt to read, edit, and delete the DoDIMS server C2 audit files.	All attempts by the root user to read, edit and delete these files are successful.			
		Restore the audit files from the backups.	Files successfully restored.			
		Login as user2 and attempt to read, edit, backup and delete the DoDIMS server C2 audit files.	All attempts to read, edit, or delete the audit files are unsuccessful.			
2.	Verify that DoDIMS application audit data should be protected from modification and unauthorized destruction	At the conclusion of security testing and after other audit tests are completed, login as ISSO and make backups of the DoDIMS application audit files	Backups successfully made.			
		Attempt to read, edit, and delete the DoDIMS application audit files.	All attempts by the root user to read, edit and delete these files are successful.			
		Restore the audit files from the backups.				

Login as user2 and attempt to read, edit, backup and delete the DoDIMS application audit files.	Files successfully restored. All attempts to read, edit, or delete the audit files are unsuccessful.

DoDIMS Audit Test Procedures
(Test 25.d.3)

.

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the system should record the following types of events: A. Use of identification and authentication mechanisms B. Actions taken by the ISSO, DoDIMS administrators and the Unix system administrators C. Use of superuser privilege login D. Change of privileges E. Other security relevant events.	At the conclusion of security testing, examine the audit data. Using the tools provided by the system.	The system should record the use of identification and authentication mechanisms, actions taken by the ISSO, user4 and system administrators, use of superuser privilege login, changes of privileges, changes to the database, and other security relevant events.			

DoDIMS Audit Test Procedure
(Test 25.d.4)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify for each DoDIMS server Unix C2 event recorded, the date and time of the event, user, type of event, and success and failure of the event is recorded. The database should be recorded.	At the conclusion of security testing, examine the DoDIMS server C2 audit data using the SunOS C2 Audit Tools.	For each event recorded, the date and time of the event, user, type of event, and success and failure of the event is recorded.			
2.	Verify for each DoDIMS application event recorded, the date and time of the event, user, type of event, and success and failure of the event is recorded. The database should be recorded.	At the conclusion of security testing, examine the DoDIMS application audit data using the VI editor.	For each event recorded, the date and time of the event, user, type of event, and success and failure of the event is recorded.			

DoDIMS System Architecture Test Procedure
(Test 25.e)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the systems ability to isolate the resources it protects from other than an authorized individual.	Review architecture plan of DoDIMS and verify only authorized users have access to DoDIMS.	Only authorized users have access to DoDIMS.			
2.	Verify the systems ability to isolate the resources it protects from access by other then an authorized terminal.	Attempt to run DoDIMS by means of a terminal not authorized.	Attempt is unsuccessful.			
3.	Verify the ability to limit system access only to authorized individuals.	Attempt to run DoDIMS as an individual without authorization.	Attempt is unsuccessful.			
4.	Verify the ability to limit system access only to authorized terminals.	Attempt to gain access to DoDIMS via an unauthorized terminal.	Attempt is unsuccessful.			

DoDIMS System Integrity Test Procedures
(Test 25.f)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the TCB maintains a domain for its own execution that protects it from external interference and tampering.	Examine system file permissions and verify permission settings.	See Appendix D.			
		Attempt to restart the system from another device (e.g. network).	System does not allow host from other source.			
2.	Verify the DoDIMS system can perform self-diagnostics each time it is started to validate the correct operation of the hardware elements of the system.	Examine system file permissions and verify the settings.	All correct hardware is identified.			
3.	Verify the DoDIMS system can perform self-diagnostics each time it is started to validate the correct operation of the firmware elements of the system.	Restart DoDIMS.	The correct copy of the OS and applications software is booted during system startup.			
4.	Verify the DoDIMS system can recover from a system crash without allowing disclosure information or unauthorized access.	Power down system. Power up system and examine audit scription and system.	All system and user files are intact			

DoDIMS Security Features User Guide Procedure
(Test 25.h)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify that the security features of the system is explained in the security Features User Guide.	Review all appropriate documents pertaining to security features which are used or encountered by the DoDIMS user.	Documentation describes the security features and instructs the user concerning them..			

DoDIMS Trusted Facility Manual Test Procedure
(Test 25.i)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify the appropriate documents and the applicable sections in each to meet this requirement to document how privileged users such as the ISSO and the System Administrator control the security features of DoDIMS and maintain and examine the audit file.	Review all appropriate documentation pertaining to control of DoDIMS security features.	Documents adequately describe how to manage DoDIMS security features.			

DoDIMS Test Documentation Test Procedure
(Test 25.j)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify that system security testing and supporting documentation is adequate.	Review DoDIMS security test documentation.	Test planning documentation should describe what security features are to be tested, how they are to be tested, and the pass/fail criteria for each test. The test report should describe the conditions of the test and actual test results. The testing should be enable the DAA to determine the degree to which the system satisfies requisite security requirements.			

DoDIMS Security Design Documentation Test Procedure
(Test 25.k)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify that design documentation describes the philosophy and functioning of security mechanisms.	Review DoDIMS system security design documentation as well as vendor documentation.	Design documentation describes how the system was designed to incorporate security mechanisms. It should describe how different functions and capabilities interface to maintain system security.			

DoDIMS Identification of Terminals Test Procedure
(Test 25.l)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify that DoDIMS can positively identify a work station attempting to mount the DoDIMS directories prior to granting access.	Attempt to mount DoDIMS directories from an unapproved workstation.	Attempt is unsuccessful			
		Attempt to mount the DoDIMS directories from an approved workstation.	Attempt is successful			

DoDIMS Configuration Management Test Procedure
(Test 25.m)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify DoDIMS compliance with requirements for a configuration management system	Review the configuration management system plan.	DoDIMS has a Configuration Management Plan			

.

DoDIMS Trusted Distribution Test Procedure
(Test 25.n)

Step	Test Activity	Operator/User Action	Pass Criteria	Results/Comments	P/F	Req.
1.	Verify that the PMO and the site have procedures that ensure trusted distribution of DoDIMS software.	Review DoDIMS PMO and site procedures for distribution and control of DoDIMS software.	Procedures provide a high degree of assurance that the software distributed by the PMO, received and installed on systems has not been tampered with.			